A new construction of (0,1)-sequenes

Shu Tezuka
Faculty of Mathematics
Kyushu University

Outline

- Low-discrepancy sequences
- Definition of (t,k)-sequences
- Polynomial analogue of generalized van der Corput sequences
- Permutations based on Fibonacci polynomials
- Discussions

Definition of Discrepancy
(A measure for uniform distribution)

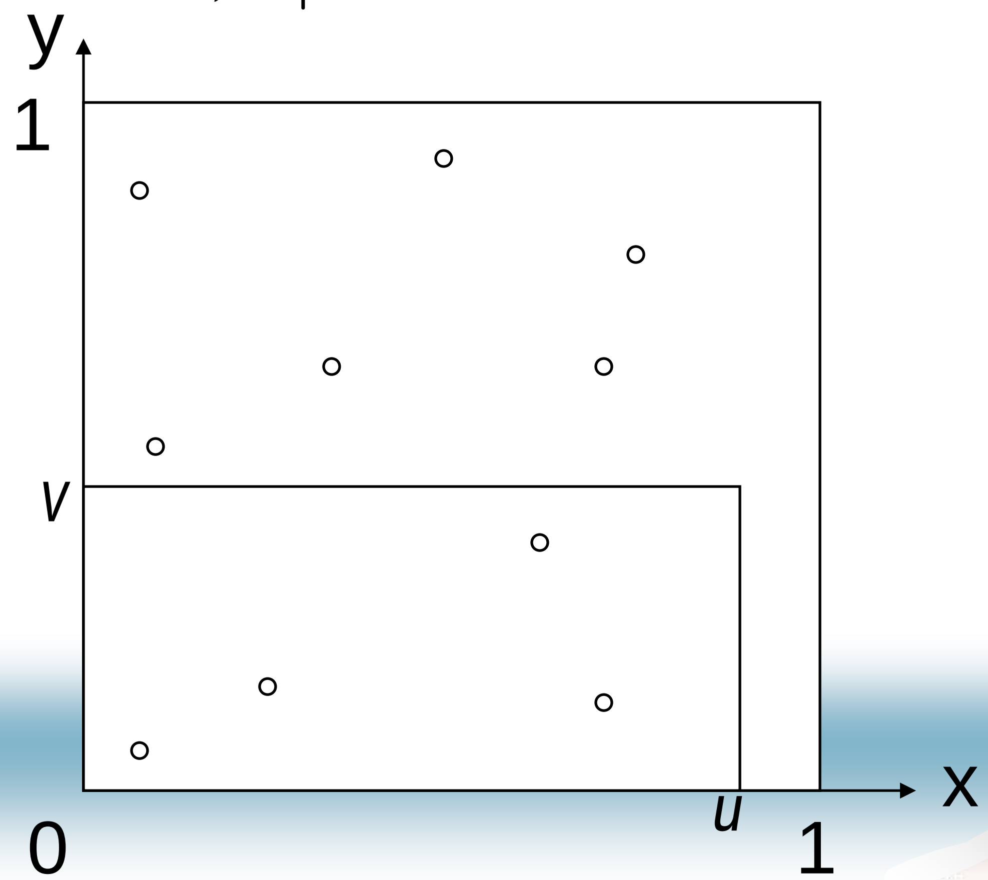
- For N points $P_i, i = 1,\ldots, N,$ in $[0,1]^k$

$$D_N^{(k)} = \sup_J \left| \frac{\#(P_i; J)}{N} - Vol(J) \right|$$

- J is the subinterval $[0, u_1) \times \cdots \times [0, u_k)$
- $\#(P_i; J)$ is the number of points in J

2-Dimensional Example

$$D_{10}^{(2)} = \sup_{0<u,v\le 1} \left| \frac{\#(P_i;[0,u)\times[0,v))}{10} - uv \right|$$



Discrepancy and Numerical Integration

- Koksma-Hlawka Theorem (1961)

$$E(f) \leq V(f) D_N^{(k)}$$

- $V(f)$: function variation and

$$E(f) = \left| \int_{[0,1]^k} f(x)dx - \frac{1}{N}\sum_{i=1}^{N} f(x_i) \right|$$

Low-Discrepancy Sequences

- Definition
  - an infinite sequence of points in $[0,1]^k$
  - For any $N > 1$, the discrepancy of the first N points of the sequence satisfies

$$D_N^{(k)} \le c_k \frac{(\log N)^k}{N}$$

Elementary Box with base b

- A b-ary box is an interval of the form

$$E = \prod_{i=1}^{k} [a_i b^{-d_i}, (a_i + 1) b^{-d_i})$$

with integers $d_i \geq 0$ and integers $0 \leq a_i < b^{d_i}$ for $1 \leq i \leq k$

(t,m,k)-nets and (t,k)-sequences

- A (t,m,k)-net with base b is a point set of points b^m such that every b-ary box of volume b^{t-m} contains exactly b^t points
- A sequence of points $X_0, X_1, \ldots$ is a (t,k)-sequence if for all integers $j \geq 0$ and $m > t$, the point set,

  $$[X_n]_m \; (jb^m \leq n < (j+1)b^m),$$

  form a (t,m,k)-net with base b.

Discrepancy of (t,k)-sequences

Niederreiter Theorem (1987)

- For any $N > 1$, the discrepancy of the first N points of the sequence satisfies

$$D_N^{(k)} \le \frac{b^t}{k!}\left(\frac{b}{2\log b}\right)^k \frac{(\log N)^k}{N} + O\left(\frac{(\log N)^{k-1}}{N}\right)$$

- If *t* is constant or dependent only on *k*, it is a low-discrepancy sequence

Construction of (t,k)-sequences

- Denote $P_i = (X_i^{(1)}, \ldots, X_i^{(k)}), i = i_1 + i_2 b + \cdots$ and
$$X_i^{(j)} = \frac{x_{i,1}^{(j)}}{b} + \cdots + \frac{x_{i,h}^{(j)}}{b^h} + \cdots (1 \le j \le k)$$
- Then
$$\begin{pmatrix} x_{i,1}^{(j)} \\ x_{i,2}^{(j)} \\ \cdots \\ \cdots \end{pmatrix} = G^{(j)} \begin{pmatrix} i_1 \\ i_2 \\ \cdots \\ \cdots \end{pmatrix}$$
- $G^{(j)} (1 \le j \le k)$ are called generator matrices

Example of (0,1)-sequences

- (t,k)-sequences with $t=0$ and $k=1$
- Van der Corput sequence: $p(z)=z$, i.e.,

$$G^{(1)} = I = \begin{pmatrix} 100 & \ldots \\ 010 & \ldots \\ 001 & \ldots \\ \ldots & \end{pmatrix},$$

- $X_i = \frac{i_1}{2} + \frac{i_2}{2^2} + \frac{i_3}{2^3} + \cdots$ for $i = i_1 + i_2 \times 2 + i_3 \times 2^2 + \cdots$

Polynomial Analogue

- An integer is replaced by a polynomial over finite fields
- A real number is replaced by a formal Laurent series over finite fields
- The arithmetic is done over finite fields

Polynomial analogue of Weyl sequences

- The original Weyl sequences is defined by

$$X_n = n\alpha \ (\mathrm{mod}\ 1)$$

- Their polynomial analogue is obtained by replacing *n* by *a polynomial*, and α by *a formal Laurent series,* then mapping it to a real number by substituting *b* into *z*

Polynomial analogue of Weyl sequences (continued)

- Analogue of Weyl sequences with respect to polynomial arithmetic over finite fields is $(t,1)$-sequences whose generator matrices are Hankel.

- (0,1)-sequences are obtained by the continued fraction expansion whose partial quotients are all of degree one, i.e., Fibonacci polynomials of degree going to infinity.

Polynomial analogue of van der Corput sequences

- Analogue of van der Corput sequence with respect to polynomial arithmetic over finite fields includes the original van der Corput sequences and another (0,1)-sequence whose generator matrix is given by

$$G = P^T P,$$

where P is the Pascal matrix.

Generalized van der Corput sequences

For a nonnegative integer $n = n_0 + n_1 b + \cdots + n_m b^m$,

generalized van der Corput sequences is defined by

$$\phi_\nu(n) = \frac{\nu(n_0)}{b} + \frac{\nu(n_1)}{b^2} + \cdots + \frac{\nu(n_m)}{b^{m+1}},$$

where ν *is a permutation on integers* $\{0,1,\ldots,b-1\}$.

An exmple of a permutation ν *is* $\nu(m) = am \pmod{b}$,

$m = 0,1,\ldots,b-1$, *where* $\gcd(a,b) = 1$.

Definition of polynomial analogue

For a nonnegative integer $n = n_0 + n_1 b + \cdots + n_m b^m$,

define $n(z) = \lambda(n_0) + \lambda(n_1)z + \cdots + \lambda(n_m)z^m$.

If $n(z) = r_0(z) + r_1(z)p(z) + \cdots + r_{s-1}(z)p(z)^{s-1}$,

then the polynomial version of generalized van der Corput sequences is defined by

$$\phi_v(n(z)) = \frac{v(r_0(z))}{p(z)} + \frac{v(r_1(z))}{p(z)^2} + \cdots + \frac{v(r_{s-1}(z))}{p(z)^s},$$

where a permutation $v(m(z)) = q(z)m(z) \pmod{p(z)}$.

Theorem

The polynomial analogue of generalized van der Corput sequences defined before is a strict (*t,1*)-sequence with

$$t = \max_{1 \le l \le \deg(p)} \left(l - \rho(H(q/p); l) \right)$$

where *H*(*q/p*) is the Hankel matrix obtained by the formal Laurent series of *q*(*z*)/*p*(*z*).

Corollary

If $p(z)$ and $q(z)$ are consecutive Fibonacci polynomials, i.e., $(q,p)=(F_{e-1},F_e)$, then the polynomial analogue of generalized van der Corput sequences defined before is a (0,1)-sequence, where $e=\deg(p)$.

Discussions

Polynomial analogue introduced here can be viewed as a hybridization of van der Corput sequences and polynomial Weyl sequences because the special case $(q,p)=(1,z)$ produces van der Corput sequences, and another special case $\deg(p)=\infty$ produces polynomial Weyl sequences.

Discussions (continued)

Thanks to Mesirov-Sweet theorem that any irreducible polynomial over GF(2) is a Fibonacci polynomial, we can construct the polynomial analogue of generalized Halton sequences over GF(2), whose coordinates are all (0,1)-sequences.